

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2002-258969
(P2002-258969A)

(43)公開日 平成14年9月13日(2002.9.13)

(51)Int.Cl. ⁷	識別記号	F I	ターム(参考)
G 0 6 F 1/00		G 0 9 C 1/00	6 4 0 D 5 B 0 7 6
9/445		G 0 6 F 9/06	6 6 0 J 5 J 1 0 4
G 0 9 C 1/00	6 4 0		6 4 0 A

審査請求 有 請求項の数13 O L (全 17 頁)

(21)出願番号 特願2001-62217(P2001-62217)

(22)出願日 平成13年3月6日(2001.3.6)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 岡田 勲

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100086759

弁理士 渡辺 喜平

Fターム(参考) 5B076 FA20 FB01 FD04

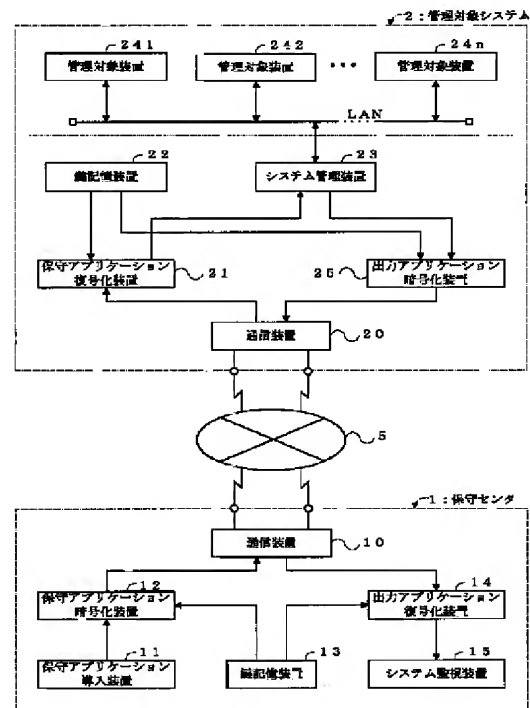
5J104 AA09 LA06 PA07

(54)【発明の名称】 分散通信システムにおける遠隔保守管理方法及びその通信システム並びにプログラム

(57)【要約】

【課題】 電子署名添付及び暗号化によって安全かつ確実な分散通信システムにおける遠隔保守管理を実施する。

【解決手段】 保守センタ1が、保守アプリケーションに対する電子署名添付及び暗号化を行って転送し、かつ、管理実施後に転送されてくる出力アプリケーションに添付されている電子署名を解析して転送元の正当性を確認し、さらに、出力アプリケーションを復号化し、出力アプリケーションを実行して保守管理のデータを得る。管理対象システム2が、保守センタ1から転送されてきた保守アプリケーションに添付されている電子署名を解析して転送元の保守センタ1の正当性を確認し、さらに、保守アプリケーションを復号化するとともに、登録して遠隔保守管理を実施し、この遠隔保守管理の実施に基づいた出力アプリケーションに対する電子署名添付及び暗号化を行って保守センタ1に転送する。



【特許請求の範囲】

【請求項1】 遠隔保守管理のための保守アプリケーション及び管理実施後の出力アプリケーションを、管理実施側及び管理対象側の装置間で転送する分散通信システムにおける遠隔保守管理方法において、管理実施側から管理対象側へ転送する保守アプリケーションに電子署名を添付して転送するステップと、この電子署名を添付した保守アプリケーションを受け取った管理対象側が、電子署名を解析して転送元である管理実施側の正当性を確認するステップと、管理対象側において正当性が確認された際に、受け取った保守アプリケーションを登録するステップと、管理対象側が登録した保守アプリケーションに基づいた遠隔保守管理を実施するステップと、を有することを特徴とする分散通信システムにおける遠隔保守管理方法。

【請求項2】 遠隔保守管理のための保守アプリケーション及び管理実施後の出力アプリケーションを、管理実施側及び管理対象側の装置間で転送する分散通信システムにおける遠隔保守管理方法において、管理対象側が保守アプリケーションに基づいて実施した遠隔保守管理による保守管理データを含む出力アプリケーションに電子署名を添付して管理実施側に転送するステップと、この電子署名を添付した管理対象側から転送された出力アプリケーションを受け取った管理実施側が電子署名を解析して転送元である管理対象側の正当性を確認するステップと、管理実施側において正当性が確認された際に、受け取った出力アプリケーションを実行して保守管理データを得るステップと、を有することを特徴とする分散通信システムにおける遠隔保守管理方法。

【請求項3】 遠隔保守管理のための保守アプリケーション及び管理実施後の出力アプリケーションを、管理実施側及び管理対象側の装置間で転送する分散通信システムにおける遠隔保守管理方法において、管理実施側から管理対象側へ転送する保守アプリケーションを暗号化して転送するステップと、この暗号化した保守アプリケーションを受け取った管理対象側が復号化するステップと、管理対象側で復号化した保守アプリケーションを登録するステップと、管理対象側が登録した保守アプリケーションに基づいた遠隔保守管理を実施するステップと、を有することを特徴とする分散通信システムにおける遠隔保守管理方法。

【請求項4】 遠隔保守管理のための保守アプリケーション及び管理実施後の出力アプリケーションを、管理実施側及び管理対象側の装置間で転送する分散通信システム

における遠隔保守管理方法において、管理対象側が保守アプリケーションに基づいて実施した遠隔保守管理による保守管理データを含む出力アプリケーションを暗号化して管理実施側に転送するステップと、この暗号化による管理対象側から転送された出力アプリケーションを受け取った管理実施側が復号化するステップと、管理実施側において復号化した出力アプリケーションを実行して実施された保守管理データを得るステップと、を有することを特徴とする分散通信システムにおける遠隔保守管理方法。

【請求項5】 遠隔保守管理のための保守アプリケーション及び管理実施後の出力アプリケーションを、管理実施側及び管理対象側の装置間で転送する分散通信システムにおける遠隔保守管理方法において、管理実施側から管理対象側へ転送する保守アプリケーションに対する電子署名添付及び／又は暗号化を行って転送するステップと、この保守アプリケーションを受け取った管理対象側が、添付されていた電子署名を解析して転送元である管理実施側の正当性を確認し、かつ、暗号化されていた保守アプリケーションを復号化するステップと、管理対象側において正当性が確認された際に保守アプリケーションを登録して遠隔保守管理を実施するステップと、この遠隔保守管理の実施に基づいた出力アプリケーションに対する電子署名添付及び／又は暗号化を管理対象側が行って管理実施側に転送するステップと、この出力アプリケーションを受け取った管理実施側が、添付されていた電子署名を解析して転送元である管理対象側の正当性を確認し、かつ、出力アプリケーションが暗号化されていた場合に復号化するステップと、管理実施側において正当性が確認された際に、受け取った出力アプリケーションを実行して保守管理のデータを得るステップと、を有することを特徴とする分散通信システムにおける遠隔保守管理方法。

【請求項6】 前記請求項1から5に記載の電子署名の確認及び暗号化として、公開鍵暗号系又は楕円暗号系を適用することを特徴とする分散通信システムにおける遠隔保守管理方法。

【請求項7】 遠隔保守管理のための保守アプリケーション及び管理実施後の出力アプリケーションを、通信手段間で転送する遠隔保守管理通信システムにおいて、保守アプリケーションに対する電子署名添付及び／又は暗号化を行って転送し、かつ、管理実施後に転送されてくる出力アプリケーションに添付されていた電子署名を解析して転送元の正当性を確認し、かつ、暗号化されていた出力アプリケーションを復号化し、出力アプリケー

ションを実行して保守管理のデータを得る保守通信手段と、

前記保守通信手段が、転送されてきた保守アプリケーションに、添付されていた電子署名を解析して転送元の保守通信手段の正当性を確認し、かつ、暗号化されていた保守アプリケーションを復号化するとともに、登録して遠隔保守管理を実施し、この遠隔保守管理の実施に基づいた出力アプリケーションに対する電子署名添付及び／又は暗号化を行って保守通信手段に転送する管理対象通信手段と、

を備えることを特徴とする遠隔保守管理通信システム。

【請求項8】 前記請求項7に記載の保守通信手段が、管理対象通信手段との通信を実行する通信装置と、当該装置の内外から保守アプリケーションを導入するための導入装置と、

前記導入装置からの保守アプリケーションを暗号化する暗号化装置と、

暗号化と復号化に必要な秘密鍵を記憶する鍵記憶部と、管理対象通信手段から転送されてきた出力アプリケーションを復号する復号化装置と、

前記復号化装置が復号化した出力アプリケーションを実行して前記管理対象通信手段からの保守管理データを出力するシステム監視装置と、

を備えることを特徴とする遠隔保守管理通信システム。

【請求項9】 前記前記請求項7に記載の管理対象通信手段が、

保守通信手段との通信を実行する通信装置と、

前記保守通信手段から転送されてきた保守アプリケーションを復号化する復号化装置と、

暗号化と復号化に必要な公開鍵及び秘密鍵を記憶する鍵記憶部と、

前記復号化装置で復号化された保守アプリケーションを送出して保守管理データの収集を行うシステム管理装置と、

前記システム管理装置から送出された保守アプリケーションを実行して前記保守通信手段の保守管理対象となる少なくとも一つの管理対象装置と、

前記管理対象装置からの出力アプリケーションを暗号化し、前記通信装置を通じて前記保守通信手段に転送するための暗号化装置と、

を備えることを特徴とする遠隔保守管理通信システム。

【請求項10】 前記請求項8又は10に記載の鍵記憶部が、

装置内部に配置された記憶装置、又は、装置の外部に配置された記憶装置として構成されることを特徴とする遠隔保守管理通信システム。

【請求項11】 前記請求項9に記載の管理対象装置が複数であり、

この複数の管理対象装置がローカルエリアネットワークを含む通信ネットワークに収容されるとともに、

この通信ネットワークとの通信接続によってシステム管理装置が保守アプリケーションを個々の管理対象装置に送出して、個々の管理対象装置が保守アプリケーションが実行した保守管理データを前記通信ネットワークに転送することを特徴とする遠隔保守管理通信システム。

【請求項12】 保守アプリケーションに対する電子署名添付及び／又は暗号化を行って転送する処理と、管理実施後に転送されてくる保守管理のデータを含む出力アプリケーションに添付されていた電子署名を解析して転送元の正当性を確認する処理と、

暗号化されていた出力アプリケーションを復号化し、出力アプリケーションを実行して保守管理のデータを得る処理と、

の制御を実質的なコンピュータが実行するためのプログラム。

【請求項13】 転送されてきた保守アプリケーションに、添付されていた電子署名を解析して転送元の保守通信手段の正当性を確認する処理と、

暗号化されていた保守アプリケーションを復号化して処理と、

復号化した保守アプリケーションを登録する処理と、

登録した復号化保守アプリケーションを実行して遠隔保守管理を実施する処理と、

この遠隔保守管理の実施に基づいた出力アプリケーションに対する電子署名添付及び／又は暗号化を行って転送する処理と、

の制御を実質的なコンピュータが実行するためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、EC(Electric Commerce)用などの分散通信システムにおける遠隔保守管理用の保守アプリケーション及び出力アプリケーションに電子署名を添付し、かつ、暗号化して転送する、分散通信システムにおける遠隔保守管理方法及びその通信システム並びにプログラムに関する。

【0002】

【従来の技術】従来、分散通信システムでは、保守管理を遠隔操作データ(遠隔保守管理用の保守アプリケーション及び出力アプリケーション)を転送して実施している(例えば、特開2000-293405号「分散システムに遠隔保守管理装置及び方法並びに該プログラムを記録した記録媒体」)。

【0003】図12は従来の分散通信システムの遠隔保守管理にかかる構成を示すブロック図である。図12を参照すると、従来の遠隔保守管理システムは、保守センタE1と管理対象システムE2から構成されている。保守センタE1は、保守アプリケーション導入装置E11及びシステム監視装置E12から構成されている。また、管理対象システムE2は、システム管理装置E21

及び管理対象装置E221, E222…E22nから構成されている。

【0004】なお、この構成では、保守センタE1と管理対象システムE2との間の通信装置や通信ネットワークの伝送系、及びシステム管理装置E21と管理対象装置E221～E22nとの間のローカルネットワーク(LAN)などの伝送系については、その図示を省略した。

【0005】このような構成の遠隔保守管理システムは、次のように動作する。まず、保守アプリケーション導入装置E11が、保守アプリケーションをシステム管理装置E21へ転送する。システム管理装置E21は保守アプリケーションを受け取り、保守管理の対象である管理対象装置E221～E22nのいずれか又は全部に時分割多重化接続などで転送する。管理対象装置E221～E22nは、転送されてきた保守アプリケーションを実行して保守処理を実施し、この保守処理で収集した保守データをシステム管理装置E21へ転送する。

【0006】システム管理装置E21は、管理対象装置E221～E22nの保守データを受け取り、この保守データを出力するための出力アプリケーションを作成して、システム監視装置E12へ転送する。システム管理装置E12は転送されてきた出力アプリケーションを実行し、保守データを画面表示する。

【0007】ところで、通信ネットワーク、特に、公衆通信ネットワークでは、転送データの暗号化が既知である。このような暗号化データ転送では、より確実な対策が必要である(例えば、特開平11-55247「送信者匿名性確保秘密情報伝達方法、その装置及びプログラム記録媒体」)。

【0008】

【発明が解決しようとする課題】しかしながら、上記従来例において、保守センタと管理対象システムとの間で保守アプリケーション及び出力アプリケーションをやり取りする分散通信システムの遠隔保守管理では、特に公衆回線網(TCP/IP通信ネットワーク/インターネット)で接続されている場合に、次のような問題が生じることがある。

【0009】(1) 保守アプリケーションを暗号化せずに転送しているため、保守アプリケーションを伝送路上で盗聴されるおそれがある。

【0010】(2) 第三者が正規の保守センタになりすまして管理対象システムに悪意ある保守アプリケーションを登録するおそれがある。それにより、管理対象システムの情報が盗まれたり、管理対象システムが破壊されたりする可能性がある。これは、保守アプリケーションが保守センタから転送されてきたものであるか否かをシステム管理装置Eが確認できないためである。

【0011】(3) 出力アプリケーションが、システム管理装置からシステム監視装置への転送中に盗聴される

おそれがある。すなわち、出力アプリケーションを暗号化せずに転送しているためである。

【0012】(4) 他人が管理対象システムになりすまして、システム監視装置へ虚偽の出力アプリケーションを転送するおそれがある。これは、出力アプリケーションが管理対象システムから転送されてきたものかを確認できないためである。

【0013】(5) このような盗聴(通信経路上での悪意あるデータ取得)、なりすまし(第三者が他人になりすましてデータ伝送を行う)とともに、悪意ある第三者による否認(通信相手先での通信の否定)、改造(通信経路上での第三者による伝送データの改変)も発生することがある。

【0014】本発明は、このような従来の技術における課題を解決するものであり、保守センタと管理対象通信システムとの間で転送する保守アプリケーション及び出力アプリケーションに電子署名を添付して、受け取り側で転送元の正当性を確認し、その安全かつ確実な遠隔保守管理を実施できる、分散通信システムにおける遠隔保守管理方法及びその通信システム並びにプログラムの提供を目的とする。

【0015】さらに、本発明は、保守センタと管理対象通信システムとの間で転送する保守アプリケーション及び出力アプリケーション(保守データ)を、暗号化して転送し、悪意の第三者による盗聴、なりすまし、否認、改造などを防止して、その安全かつ確実な遠隔保守管理を実施できる、分散通信システムにおける遠隔保守管理方法及びその通信システム並びにプログラムの提供を他の目的とする。

【0016】

【課題を解決するための手段】上記課題を達成するために、本発明の分散通信システムにおける遠隔保守管理方法は、遠隔保守管理のための保守アプリケーション及び管理実施後の出力アプリケーションを、管理実施側及び管理対象側の装置間で転送するものであり、管理実施側から管理対象側へ転送する保守アプリケーションに電子署名を添付して転送するステップと、この電子署名を添付した保守アプリケーションを受け取った管理対象側が、電子署名を解析して転送元である管理実施側の正当性を確認するステップと、管理対象側において正当性が確認された際に、受け取った保守アプリケーションを登録するステップと、管理対象側が登録した保守アプリケーションに基づいた遠隔保守管理を実施するステップとを有している。

【0017】本発明の方法は、遠隔保守管理のための保守アプリケーション及び管理実施後の出力アプリケーションを、管理実施側及び管理対象側の装置間で転送するものであり、管理対象側が保守アプリケーションに基づいて実施した遠隔保守管理による保守管理データを含む出力アプリケーションに電子署名を添付して管理実施側

に転送するステップと、この電子署名を添付した管理対象側から転送された出力アプリケーションを受け取った管理実施側が電子署名を解析して転送元である管理対象側の正当性を確認するステップと、管理実施側において正当性が確認された際に、受け取った出力アプリケーションを実行して保守管理データを得るステップとを有している。

【0018】本発明の方法は、遠隔保守管理のための保守アプリケーション及び管理実施後の出力アプリケーションを、管理実施側及び管理対象側の装置間で転送するものであり、管理実施側から管理対象側へ転送する保守アプリケーションを暗号化して転送するステップと、この暗号化した保守アプリケーションを受け取った管理対象側が復号化するステップと、管理対象側で復号化した保守アプリケーションを登録するステップと、管理対象側が登録した保守アプリケーションに基づいた遠隔保守管理を実施するステップとを有している。

【0019】本発明の方法は、遠隔保守管理のための保守アプリケーション及び管理実施後の出力アプリケーションを、管理実施側及び管理対象側の装置間で転送するものであり、管理対象側が保守アプリケーションに基づいて実施した遠隔保守管理による保守管理データを含む出力アプリケーションを暗号化して管理実施側に転送するステップと、この暗号化による管理対象側から転送された出力アプリケーションを受け取った管理実施側が復号化するステップと、管理実施側において復号化した出力アプリケーションを実行して実施された保守管理データを得るステップとを有している。

【0020】本発明の方法は、遠隔保守管理のための保守アプリケーション及び管理実施後の出力アプリケーションを、管理実施側及び管理対象側の装置間で転送するものであり、管理実施側から管理対象側へ転送する保守アプリケーションに対する電子署名添付及び／又は暗号化を行って転送するステップと、この保守アプリケーションを受け取った管理対象側が、添付されていた電子署名を解析して転送元である管理実施側の正当性を確認し、かつ、暗号化されていた保守アプリケーションを復号化するステップと、管理対象側において正当性が確認された際に保守アプリケーションを登録して遠隔保守管理を実施するステップと、この遠隔保守管理の実施に基づいた出力アプリケーションに対する電子署名添付及び／又は暗号化を管理対象側が行って管理実施側に転送するステップと、この出力アプリケーションを受け取った管理実施側が、添付されていた電子署名を解析して転送元である管理対象側の正当性を確認し、かつ、出力アプリケーションが暗号化されていた場合に復号化するステップと、管理実施側において正当性が確認された際に、受け取った出力アプリケーションを実行して保守管理のデータを得るステップとを有している。

【0021】本発明の方法は、前記電子署名の確認及び

暗号化として、公開鍵暗号系又は慣用暗号系を適用している。

【0022】本発明の遠隔保守管理通信システムは、遠隔保守管理のための保守アプリケーション及び管理実施後の出力アプリケーションを、通信手段間で転送するものであり、保守アプリケーションに対する電子署名添付及び／又は暗号化を行って転送し、かつ、管理実施後に転送されてくる出力アプリケーションに添付されていた電子署名を解析して転送元の正当性を確認し、かつ、暗号化されていた出力アプリケーションを復号化し、出力アプリケーションを実行して保守管理のデータを得る保守通信手段と、前記保守通信手段が、転送されてきた保守アプリケーションに、添付されていた電子署名を解析して転送元の保守通信手段の正当性を確認し、かつ、暗号化されていた保守アプリケーションを復号化するとともに、登録して遠隔保守管理を実施し、この遠隔保守管理の実施に基づいた出力アプリケーションに対する電子署名添付及び／又は暗号化を行って保守通信手段に転送する管理対象通信手段とを備える構成としてある。

【0023】本発明の通信システムは、前記保守通信手段が、管理対象通信手段との通信を実行する通信装置と、当該装置の内外から保守アプリケーションを導入するための導入装置と、前記導入装置からの保守アプリケーションを暗号化する暗号化装置と、暗号化と復号化に必要な秘密鍵を記憶する鍵記憶部と、管理対象通信手段から転送されてきた出力アプリケーションを復号する復号化装置と、前記復号化装置が復号化した出力アプリケーションを実行して前記管理対象通信手段からの保守管理データを出力するシステム監視装置とを備える構成としてある。

【0024】本発明の通信システムは、前記前記管理対象通信手段が、保守通信手段との通信を実行する通信装置と、前記保守通信手段から転送されてきた保守アプリケーションを復号化する復号化装置と、暗号化と復号化に必要な公開鍵及び秘密鍵を記憶する鍵記憶部と、前記復号化装置で復号化された保守アプリケーションを送出して保守管理データの収集を行うシステム管理装置と、前記システム管理装置から送出された保守アプリケーションを実行して前記保守通信手段の保守管理対象となる少なくとも一つの管理対象装置と、前記管理対象装置からの出力アプリケーションを暗号化し、前記通信装置を通じて前記保守通信手段に転送するための暗号化装置とを備える構成としてある。

【0025】本発明の通信システムは、前記請求項8又は10の遠隔保守管理通信システムに記載の鍵記憶部が、装置内部に配置された記憶装置、又は、装置の外部に配置された記憶装置として構成されている。

【0026】本発明の通信システムは、前記管理対象装置が複数であり、この複数の管理対象装置がローカルエリアネットワークを含む通信ネットワークに収容される

とともに、この通信ネットワークとの通信接続によってシステム管理装置が保守アプリケーションを個々の管理対象装置に送出して、個々の管理対象装置が保守アプリケーションが実行した保守管理データを前記通信ネットワークに転送する構成としてある。

【0027】本発明のプログラムは、保守アプリケーションに対する電子署名添付及び／又は暗号化を行って転送する処理と、管理実施後に転送されてくる保守管理データを含む出力アプリケーションに添付されていた電子署名を解析して転送元の正当性を確認する処理と、暗号化されていた出力アプリケーションを復号化し、出力アプリケーションを実行して保守管理データを得る処理との制御を実質的なコンピュータが実行するものである。

【0028】本発明のプログラムは、転送されてきた保守アプリケーションに、添付されていた電子署名を解析して転送元の保守通信手段の正当性を確認する処理と、暗号化されていた保守アプリケーションを復号化して処理と、復号化した保守アプリケーションを登録する処理と、登録した復号化保守アプリケーションを実行して遠隔保守管理を実施する処理と、この遠隔保守管理の実施に基づいた出力アプリケーションに対する電子署名添付及び／又は暗号化を行って転送する処理との制御を実質的なコンピュータが実行するものである。

【0029】このような本発明は、EC (Electric Commerce) 用などの分散通信システムにおける遠隔保守管理において、保守センタと管理対象通信システムとの間で転送する保守アプリケーション及び出力アプリケーションに電子署名を添付している。したがって、転送途中のデータ改変を検証できるようになる。すなわち、転送元の正当性が確認されて、その安全で正しい保守アプリケーション及び出力アプリケーションの受け取りが可能になる。

【0030】さらに、本発明は、EC (Electric Commerce) 用などの分散通信システムにおける遠隔保守管理において、保守センタと管理対象通信システムとの間で転送する保守アプリケーション及び出力アプリケーション（保守管理データ）を、暗号化して安全に転送している。したがって、転送路上での解読が容易には出来ない。したがって、悪意の第三者による盗聴、なりすまし、否認、改造などが確実に阻止される。

【0031】

【発明の実施の形態】次に、本発明の分散通信システムにおける遠隔保守管理方法及びその通信システム並びにプログラムの実施の形態を図面参照して詳細に説明する。図1は本発明の実施形態における構成を示すブロック図である。

【0032】図1において、この例は、保守通信手段としての保守センタ1が管理対象通信手段としての管理対象システム2を遠隔保守管理する構成である。保守センタ1と管理対象システム2とは、ローカルエリアネット

ワーク (LAN) やTCP/IP (Transmission Control Protocol/Internet Protocol) 環境下の通信ネットワーク (例えば、イントラネット、インターネット、エキストラネット、UNIX (登録商標) ワークステーション) で接続されている。以下、この保守センタ1と管理対象システム2との間における暗号化方式として公開鍵暗号系 (public key encryption/RSA, MH) を適用して説明する。

【0033】保守センタ1は、通信装置10と、保守アプリケーションを導入するための保守アプリケーション導入装置11と、保守アプリケーションを暗号化するための保守アプリケーション暗号化装置12と、暗号化と復号化に必要な公開鍵及び秘密鍵を記憶する装置内部に配置された記憶装置としての鍵記憶部13と、管理対象システム2から転送されてくる出力アプリケーションを復号するための出力アプリケーション復号化装置14と、出力アプリケーションを実行して保守データを出力するシステム監視装置15から構成されている。

【0034】管理対象システム2は、通信装置20と、保守センタ1から転送されてくる保守アプリケーションを復号するための保守アプリケーション復号化装置21と、暗号化と復号化に必要な公開鍵及び秘密鍵を記憶する鍵記憶部22と、保守アプリケーションの配布と保守データの収集を行うシステム管理装置23と、管理対象の装置である管理対象装置241～24nと、出力アプリケーションを暗号化するための出力アプリケーション暗号化装置25から構成されている。

【0035】保守センタ1において、保守アプリケーション導入装置11は、管理対象システム2で動作させる保守アプリケーションを入力する。鍵記憶装置13は、電子署名と暗号化に必要な保守センタ1の秘密鍵と公開鍵、及び、管理対象システム241～24nの公開鍵を記憶している。また、保守アプリケーション暗号化装置12は、保守アプリケーション導入装置11に入力された保守アプリケーションに対して、鍵記憶装置13に記憶されている保守センタ1の秘密鍵を用いて電子署名を添付し、さらに、鍵記憶装置13に記憶されている管理対象システム2の公開鍵を用いて暗号化して、管理対象システム2へ転送する。

【0036】このように、保守アプリケーションを暗号化して転送すると、転送途中の通信経路で保守アプリケーションのデータが盗まれたとしても、解読されるおそれが少ない。

【0037】図1において、出力アプリケーション復号化装置14は、管理対象システム2から転送されてきた暗号化された出力アプリケーションを受け取って、鍵記憶装置13に記憶されている保守センタ1の秘密鍵を用いて復号化し、鍵記憶装置13に記憶されている管理対象システム241～24nの公開鍵を用いて、添付されている電子署名の認証を行う。

【0038】この認証に失敗した場合は、出力アプリケーションが管理対象システム241～24n以外の第三者から転送されてきたものである確率が高いため処理を中断する。

【0039】このように出力アプリケーションの出所を確認することができるため、管理対象システム241～24nになりすました第三者からの悪意ある出力アプリケーションの転送を防止できる。

【0040】図1において、管理対象システム2中の鍵記憶装置22は、電子署名と暗号化に必要な管理対象システム241～24nのそれぞれの秘密鍵と公開鍵、及び、保守センタ1の公開鍵を記憶している。保守アプリケーション復号化装置21は、保守センタ1から転送されてきた暗号化された保守アプリケーションを受け取り、鍵記憶装置22に記憶されている管理対象システム241～24nの秘密鍵を用いて復号化し、鍵記憶装置22に記憶されている保守センタ1の公開鍵を用いて、添付されている電子署名の認証を行う。認証に失敗した場合には、保守アプリケーションが保守センタ1以外の第三者から転送されてきたものである確率が高いため、処理を中断する。

【0041】このように保守アプリケーションの出所を確認することができるため、保守センタ1になりすました第三者から悪意ある保守アプリケーションが送り付けられることを防止できる。

【0042】図1において、管理対象システム2中のシステム管理装置23は、管理対象の装置である管理対象装置241～24nを統合管理するためのものである。システム管理装置23は、保守アプリケーション復号化装置21によって保守アプリケーションを取得し、管理対象装置241～24nに対して保守アプリケーションを配布し、その実行結果である保守データを管理対象装置241～24nから取得して、保守データからデータを出力するための出力アプリケーションを作成する。

【0043】また、出力アプリケーション暗号化装置25は、システム管理装置23で作成された出力アプリケーションに対して、鍵記憶装置22に記憶されている管理対象システム241～24nそれぞれの秘密鍵を用いて電子署名を添付し、さらに、鍵記憶装置22に記憶されている保守センタ1の公開鍵を用いて暗号化して、保守センタ1へ転送する。

【0044】このように出力アプリケーションも暗号化して転送するため、転送途中の通信経路で出力アプリケーションのデータが盗まれたとしても、解読される恐れが少ない。

【0045】システム監視装置15は、出力アプリケーション復号化装置14から出力アプリケーションを取得し、出力アプリケーションを実行して、保守データを出力する。

【0046】図2は、図1に示す各部の詳細な構成を示

すブロック図である。図1及び図2において、保守アプリケーション導入装置11は、アプリケーション動作手段111を有している。アプリケーション動作手段111は、保守アプリケーションを入力するためのアプリケーションを動作させて、指定された保守アプリケーションを読み込み、保守アプリケーション暗号化装置12へ転送する。

【0047】鍵記憶装置13は、鍵記憶部131と公開鍵記憶部132とを有している。鍵記憶部131は、保守センタ1の公開鍵と秘密鍵を記憶している。公開鍵記憶部132は、保守センタが管理している管理対象システム241～24nそれぞれの公開鍵を記憶している。

【0048】保守アプリケーション暗号化装置12は、ネットワークなどにより管理対象システム2と接続しており、保守アプリケーション電子署名添付手段121と、保守アプリケーション暗号化手段122を有している。保守アプリケーション電子署名添付手段121は、鍵記憶部131から保守センタの公開鍵を取得し、保守アプリケーションに電子署名を添付する。保守アプリケーション暗号化手段122は、公開鍵記憶部132から転送先の管理対象システム2の公開鍵を取得し、保守アプリケーションを暗号化する。そして、暗号化した保守アプリケーションと電子署名を管理対象システム2に転送する。

【0049】出力アプリケーション復号化装置14は、ローカルエリアネットワークで管理対象システム2と接続されており、出力アプリケーション復号化手段142と、出力アプリケーション電子署名確認手段141を有している。出力アプリケーション復号化手段142は、管理対象システム2から転送されてくる暗号化された出力アプリケーションと電子署名を受け取り、鍵記憶部131から保守センタの秘密鍵を取得して、出力アプリケーションを復号化する。出力アプリケーション電子署名確認手段141は、出力アプリケーション復号化手段142から出力アプリケーションと電子署名を受け取り、公開鍵記憶部132から管理対象システム2の公開鍵を取得して、電子署名の認証を行う。そして、認証に成功すると、システム監視装置15に出力アプリケーションを転送する。

【0050】システム監視装置15は、アプリケーション動作手段151を有している。アプリケーション動作手段151は、出力アプリケーション電子署名確認手段141から転送されてきた出力アプリケーションを動作させ、保守データを表示する。

【0051】図2において、鍵記憶装置22は、公開鍵記憶部221と鍵記憶部222とを有している。公開鍵記憶部221は、保守センタの公開鍵を記憶している。鍵記憶部222は、管理対象システム241～24nの公開鍵と秘密鍵を記憶している。

【0052】保守アプリケーション復号化装置21は、

ネットワークなどにより保守センタ1と接続しており、保守アプリケーション復号化手段211と、保守アプリケーション電子署名確認手段212とを有している。保守アプリケーション復号化手段211は、保守アプリケーション暗号化手段122から転送されてくる暗号化された保守アプリケーションと電子署名を受け取り、鍵記憶部222から管理対象システム241～24nの秘密鍵を取得して、保守アプリケーションを復号化する。保守アプリケーション電子署名確認手段212は、保守アプリケーション復号化手段211から保守アプリケーションと電子署名を受け取り、公開鍵記憶部222から保守センタの公開鍵を取得して、電子署名の認証を行う。そして、認証に成功すると、システム管理装置23に保守アプリケーションを転送する。

【0053】図2において、システム管理装置23は、保守アプリケーション登録手段231と出力アプリケーション作成手段232を有している。保守アプリケーション登録手段231は、保守アプリケーション電子署名確認手段212から転送されてくる保守アプリケーションを受け取り、管理対象装置241～24nへ転送する。管理対象装置241～24nは保守アプリケーションを実行して、実行結果である保守データを出力アプリケーション作成手段232へ転送する。出力アプリケーション作成手段232は、保守データからデータを出力するための出力アプリケーションを作成し、出力アプリケーション暗号化装置25へ転送する。

【0054】図2において、出力アプリケーション暗号化装置25は、出力アプリケーション電子署名添付手段251と、出力アプリケーション暗号化手段252とを有している。出力アプリケーション電子署名添付手段251は、出力アプリケーション作成手段232から転送されてくる出力アプリケーションを受け取り、鍵記憶部222から管理対象システム241～24nの秘密鍵を取得して、出力アプリケーションに電子署名を添付する。出力アプリケーション暗号化手段252は、公開鍵記憶部221から保守センタの公開鍵を取得して、出力アプリケーションを暗号化する。そして、暗号化した出力アプリケーションと電子署名を保守センタ1に転送する。

【0055】以下、実施形態の詳細な動作について説明する。まず、保守アプリケーションの登録動作について説明する。図3は保守アプリケーションの登録動作の処理手順を示すフローチャートである。図1から図3において、保守アプリケーションの登録動作では、まず、保守アプリケーション導入装置11が、入力アプリケーションをアプリケーション動作手段111で実行し、保守アプリケーションを取得する(図3のステップS1)。

【0056】次に、保守アプリケーション電子署名添付手段121は、鍵記憶部131から保守センタの秘密鍵を取得する(ステップS2)。そして、保守アプリケー

ション電子署名添付手段121は、取得した秘密鍵を用いて保守アプリケーションに電子署名を添付する(ステップS3)。

【0057】次に、保守アプリケーション暗号化手段122は、公開鍵記憶部132から転送先の管理対象システム2の公開鍵を取得する(ステップS4)。次に、保守アプリケーション暗号化手段122は、取得した公開鍵を用いて保守アプリケーションを暗号化する(ステップS5)。さらに、保守アプリケーション暗号化手段122は、暗号化した保守アプリケーションとステップS3で作成した電子署名を管理対象システム2へ転送する(ステップS6)。

【0058】次に、保守アプリケーション復号化手段211は、鍵記憶部222から管理対象システム2の秘密鍵を取得する(ステップS7)。次に、保守アプリケーション復号化手段211は、取得した秘密鍵を用いて保守センタ1から転送されてきた保守アプリケーションを復号化する(ステップS8)。

【0059】次に、保守アプリケーション電子署名確認手段212は、公開鍵記憶部221から保守センタの公開鍵を取得する(ステップS9)。次に、保守アプリケーション電子署名確認手段212は、取得した公開鍵を用いて保守センタ1から転送されてきた電子署名の認証を行う(ステップS10)。電子署名が正しくなければ処理を終了する(ステップS11)。電子署名が正しければ、保守アプリケーション電子署名確認手段212、保守アプリケーション登録手段231保守アプリケーションを転送し、保守アプリケーションの登録を実行して終了となる(ステップS12)。

【0060】次に、出力アプリケーションの転送動作について説明する。図4は出力アプリケーションの転送動作の処理手順を示すフローチャートである。図1、図2及び図4において、出力アプリケーション作成手段232は、管理対象装置241～24nで保守アプリケーションを実行した結果で収集された保守データからデータ出力用の出力アプリケーションを作成する(図4のステップS21)。

【0061】次に、出力アプリケーション電子署名添付手段251は、鍵記憶部222から管理対象システム241～24nの秘密鍵を取得する(ステップS22)。次に、出力アプリケーション電子署名添付手段251は、取得した秘密鍵を用いて出力アプリケーションに電子署名を添付する(ステップS23)。

【0062】次に、出力アプリケーション暗号化手段252は、公開鍵記憶部221から保守センタ1の公開鍵を取得する(ステップS24)。次に、出力アプリケーション暗号化手段252は、取得した公開鍵を用いて出力アプリケーションを暗号化する(ステップS25)。次に、出力アプリケーション暗号化手段252は、暗号化した出力アプリケーションとステップS23で作成し

た電子署名を保守センタ1へ転送する（ステップS26）。

【0063】次に、出力アプリケーション復号化手段142は、鍵記憶部131から保守センタ1の秘密鍵を取得する（ステップS27）。次に、出力アプリケーション復号化手段142は、取得した秘密鍵を用いて管理対象システム2から転送されてきた出力アプリケーションを復号化する（ステップS28）。

【0064】次に、出力アプリケーション電子署名確認手段141は、公開鍵記憶部132から転送元の管理対象システム2の公開鍵を取得する（ステップS29）。次に、出力アプリケーション電子署名確認手段141は、取得した公開鍵を用いて管理対象システム2から転送されてきた電子署名の認証を行う（ステップS30）。正しくなければ処理を終了する（ステップS31）。電子署名が正しければ出力アプリケーション電子署名確認手段141が、システム監視装置15へ出力アプリケーションを転送する。アプリケーション動作手段151は出力アプリケーション実行し、保守データを出力して終了となる（ステップS32）。

【0065】次に、実施形態の動作を、より具体的に説明する。図5は保守アプリケーション登録動作を詳細に説明するための図である。なお、括弧内のステップ番号は図3に対応する。最初に、保守アプリケーション導入装置11に保守アプリケーションC1が入力される（ステップS1）。

【0066】次に、保守アプリケーション暗号化装置12は、鍵記憶部131から保守センタの秘密鍵C3を取得する（ステップS2）。保守アプリケーション暗号化装置12は、保守アプリケーションC1からHash値C2を計算し、このHash値C2を保守センタの秘密鍵C3で暗号化することによって、電子署名C5を作成する（ステップS3）。保守アプリケーション暗号化装置12は、公開鍵記憶部132から転送先の管理対象システムAの公開鍵C6を取得する（ステップS4）。

【0067】保守アプリケーション暗号化装置12は、保守アプリケーションC1を管理対象システムAの公開鍵C6で暗号化することにより、暗号化保守アプリケーションC8を作成する（ステップS5）。保守アプリケーション暗号化装置12は、作成した暗号化保守アプリケーションC8と電子署名C5を管理対象システムAに転送する（ステップS6）。

【0068】保守アプリケーション復号化装置21は、鍵記憶部222から管理対象システムAの秘密鍵C9を取得する（ステップS7）。保守アプリケーション復号化装置21は、保守センタ1から転送されてきた暗号化保守アプリケーションC8を管理対象システムAの秘密鍵C9で復号化して、保守アプリケーションC10を作成する（ステップS8）。保守アプリケーション復号化装置21は、公開鍵記憶部221から保守センタの公開

鍵C4を取得する（ステップS9）。保守アプリケーション復号化装置21は、保守センタ1から転送されてきた電子署名C5を保守センタの公開鍵C4で復号化して、Hash値C11を取得する。

【0069】さらに、保守アプリケーション復号化装置21は、復号化した保守アプリケーションC10からHash値C12を計算し、Hash値C11と比較する（ステップS10）。Hash値C11とHash値C12が等しければ電子署名は正しいと判断し（ステップS11）、保守アプリケーションC10をシステム管理装置23に転送して、登録を行う（ステップS12）。Hash値C11とHash値C12が異なれば電子署名は不正であると判断し（ステップS11）、その処理を中止する。

【0070】次に、出力アプリケーションの転送動作を詳細に説明する。図6は出力アプリケーションの転送動作を詳細に説明するための図である。なお、括弧内のステップ番号は図4に対応する。最初に、システム管理装置23は、管理対象装置241～24nで保守アプリケーションを実行した結果集まった保守データからデータを出力するための出力アプリケーションD1を作成する（ステップS21）。

【0071】次に、出力アプリケーション暗号化装置25は、鍵記憶部222から管理対象システムAの秘密鍵C9を取得する（ステップS22）。出力アプリケーション暗号化装置25は、出力アプリケーションD1からHash値D2を計算し、Hash値D2を保守センタの秘密鍵C9で暗号化することにより、電子署名D3を作成する（ステップS23）。

【0072】出力アプリケーション暗号化装置25は、公開鍵記憶部221から保守センタの公開鍵C4を取得する（ステップS24）。出力アプリケーション暗号化装置25は、出力アプリケーションD1を保守センタの公開鍵C4で暗号化することにより、暗号化出力アプリケーションD4を作成する（ステップS25）。出力アプリケーション暗号化装置25は、作成した暗号化出力アプリケーションD4と電子署名D3を保守センタに転送する（ステップS26）。

【0073】出力アプリケーション復号化装置14は、鍵記憶部131から保守センタの秘密鍵C3を取得する（ステップS27）。出力アプリケーション復号化装置14は、管理対象システムAから転送されてきた暗号化出力アプリケーションD4を保守センタの秘密鍵C3で復号化して、出力アプリケーションD5を作成する（ステップS28）。

【0074】出力アプリケーション復号化装置14は、公開鍵記憶部132から管理対象システム1の公開鍵C6を取得する（ステップS29）。出力アプリケーション復号化装置14は、管理対象システムから転送されてきた電子署名D3を管理対象システムAの公開鍵C6で

復号化してH a s h値D 6を取得する。さらに、出力アプリケーション復号化装置1 4は、復号化した出力アプリケーションD 5からH a s h値D 7を計算してH a s h値D 6と比較する(ステップS 3 0)。

【0075】H a s h値D 6とH a s h値D 7が等しければ電子署名は正しいと判断し(ステップS 3 1)、出力アプリケーションD 5をシステム監視装置1 5に転送して、保守データの出力を実行する(ステップS 3 2)。H a s h値D 6とH a s h値D 7が異なれば電子署名は不正であると判断し(ステップS 3 1)、その処理を中止する。

【0076】次に、他の実施形態を図面参照して詳細に説明する。他の実施形態において、前記した図1から図6と同様の構成要素には、同一の参照符号を付した。図7は他の実施形態の詳細な構成を示すブロック図である。図7の他の実施形態は、図2に示した構成に加えて公開鍵記憶装置3を有している。一方、鍵記憶装置1 3には、図2に示した公開鍵記憶部1 3 2が設けられておらずまた、鍵記憶装置2 2にも公開鍵記憶部2 2 1は設けられていない。

【0077】図7を参照すると、公開鍵記憶装置3は、保守センタ1及び管理対象システム2の両方に対する公開鍵を管理するための装置であり、装置の外部に配置された記憶装置としての公開鍵記憶部3 1を有している。この公開鍵記憶部3 1は、当該装置において管理するすべての管理対象システム2 4 1～2 4 nの公開鍵と、保守センタ1の公開鍵を記憶している。

【0078】次に、他の実施形態の動作について説明する。図8は他の実施形態における保守アプリケーションの登録動作の処理手順を示すフローチャートである。図7及び図8において、図8のステップS 4 1からステップS 4 3までの動作は、図3のステップS 1からステップS 3と同様の処理であり、重複した説明は省略する。保守アプリケーション暗号化装置1 2の保守アプリケーション暗号化手段1 2 2は、保守アプリケーションを暗号化するために必要となる管理対象システム2 4 1～2 4 nの公開鍵を公開鍵記憶装置3の公開鍵記憶部3 1から取得する(図8のステップS 4 4)。

【0079】図8中のステップS 4 5からステップS 4 8までの動作は、図3のステップS 5からステップS 8と同様の処理であり、重複した説明は省略する。保守アプリケーション復号化装置2 1の保守アプリケーション電子署名確認手段2 1 2は、電子署名を認証するために必要となる保守センタの公開鍵を、公開鍵記憶装置3の公開鍵記憶部3 1から取得する(ステップS 4 9)。図8中のステップS 5 0からステップS 5 2までの動作は、図3のステップS 1 0からステップS 1 2と同様の処理であり、重複した説明は省略する。

【0080】次に、他の実施形態の動作について説明する。図9は他の実施形態における出力アプリケーション

の転送動作の処理手順を示すフローチャートである。図7及び図9において、図9中のステップS 6 1からステップS 6 3までの動作は、図4のステップS 2 1からステップS 2 3と同様の処理であり、重複した説明は省略する。

【0081】図7中の出力アプリケーション暗号化装置2 5の出力アプリケーション暗号化手段2 5 2は、出力アプリケーションを暗号化するために必要となる保守センタの公開鍵を公開鍵記憶装置3の公開鍵記憶部3 1から取得する(ステップS 6 4)。図9中のステップS 6 5からステップS 6 8までの動作は、図4のステップS 2 5からステップS 2 8と同様の処理であり、重複した説明は省略する。

【0082】図7中の出力アプリケーション復号化装置1 4の保守アプリケーション電子署名確認手段1 4 1は、電子署名を認証するために必要となる管理対象システム2 4 1～2 4 nそれぞれの公開鍵を、公開鍵記憶装置3の公開鍵記憶部3 1から取得する(ステップS 6 9)。図9中のステップS 7 0からステップS 7 2までの動作は、図4のステップS 3 0からステップS 3 2と同様の処理であり、重複した説明は省略する。

【0083】次に、他の実施形態の具体的な動作について説明する。図10は保守アプリケーション登録動作の具体的な動作を説明するための図である。図10の具体例では、前記した図5の具体例において、公開鍵記憶部1 3 2に記憶していた管理対象システムAの公開鍵C 6、及び管理対象システムBの公開鍵C 7、さらに、公開鍵記憶部2 2 1に記憶していた保守センタ1の公開鍵C 4が、それぞれ公開鍵記憶装置3の公開鍵記憶部3 1に記憶されている。図10中のステップS 4 1からステップS 4 3までの動作は、図5の具体例のステップS 1から図3までの動作と同様であり、重複した説明は省略する。

【0084】図10において、保守アプリケーション暗号化装置1 2は、保守アプリケーションC 1の転送先である管理対象システムAの公開鍵C 6を公開鍵記憶装置3の公開鍵記憶部3 1から取得する(ステップS 4 4)。図10中のステップS 4 5からステップS 4 8までの動作は、図5の具体例のステップS 5からステップS 8までの動作と同様であり、重複した説明は省略する。

【0085】図10において、保守アプリケーション復号化装置2 1は、電子署名を認証するために必要となる保守センタの公開鍵C 4を、公開鍵記憶装置3の公開鍵記憶部3 1から取得する(ステップS 4 9)。図10中のステップS 5 0からステップS 5 2までの動作は、図5の具体例のステップS 1 0からステップS 1 2までの動作と同様であり、重複した説明は省略する。

【0086】次に、他の実施形態の動作について説明する。図11は出力アプリケーション転送動作の具体的な

動作を説明するための図である。図11の具体例は、図6の具体例が公開鍵記憶部132に記憶していた管理対象システムAの公開鍵C6と管理対象システムBの公開鍵C7及び公開鍵記憶部221に記憶していた保守センタの公開鍵C4が、公開鍵記憶装置3の公開鍵記憶部31に記憶されている点で異なる。

【0087】図11におけるステップS61からステップS63までの動作は、図6の具体例のステップS21からステップS23までの動作と同様であり、重複した説明は省略する。図10において、出力アプリケーション暗号化装置25は、出力アプリケーションD1を暗号化するために必要となる保守センタの公開鍵C4を公開鍵記憶装置3の公開鍵記憶部31から取得する（ステップS64）。

【0088】図11におけるステップS65からステップS68までの動作は、図6の具体例のステップS25からステップS28までの動作と同様であり、重複した説明は省略する。出力アプリケーション復号化装置14は、電子署名を認証するために必要となる管理対象システムAの公開鍵C6を、公開鍵記憶装置3の公開鍵記憶部31から取得する（ステップS69）。図11におけるステップS70からステップS72までの動作は、図6の具体例のステップS30からステップS32までの動作と同様であり、重複した説明は省略する。

【0089】なお、前記した実施形態では、公開鍵暗号系を適用して説明したが、これに限定されない。例えば、暗号化と復号化に同一鍵を使用し、文字の順序の変更（転字）と文字の変更（換字）を行うDES、DEA1による慣用暗号系（conventional encryption system）でも、同様の作用効果が得られる。

【0090】

【発明の効果】以上の説明から明らかなように、本発明の分散通信システムにおける遠隔保守管理方法及びその通信システム並びにプログラムによれば、分散通信システムにおける遠隔保守管理において、保守センタと管理対象通信システムとの間で転送する保守アプリケーション及び出力アプリケーションに電子署名を添付している。

【0091】この結果、転送途中のデータ改変を検証できるようになり、その転送元の正当性が確認されて、安全で正しい保守アプリケーション及び出力アプリケーションの受け取りが可能になり、安全かつ確実な分散通信システムにおける遠隔保守管理を実施できるという効果を有している。

【0092】さらに、本発明によれば、EC用などの分散通信システムにおける遠隔保守管理において、保守センタと管理対象通信システムとの間で転送する保守アプリケーション及び保守データを、暗号化して転送してい

る。

【0093】この結果、転送路上での解読が容易にはできず、その悪意の第三者による盗聴、なりすまし、否認、改造などが確実に阻止されて、安全かつ確実な分散通信システムにおける遠隔保守管理が実施できるという効果を有している。

【図面の簡単な説明】

【図1】本発明の実施形態における構成を示すブロック図である。

【図2】図1に示す各部の詳細な構成を示すブロック図である。

【図3】実施形態にあって保守アプリケーションの登録動作の処理手順を示すフローチャートである。

【図4】実施形態にあって出力アプリケーションの転送動作の処理手順を示すフローチャートである。

【図5】実施形態にあって保守アプリケーション登録動作を詳細に説明するための図である。

【図6】実施形態にあって出力アプリケーションの転送動作を詳細に説明するための図である。

【図7】他の実施形態の詳細な構成を示すブロック図である。

【図8】他の実施形態における保守アプリケーションの登録動作の処理手順を示すフローチャートである。

【図9】他の実施形態における出力アプリケーションの転送動作の処理手順を示すフローチャートである。

【図10】実施形態にあって保守アプリケーション登録動作の具体的な動作を説明するための図である。

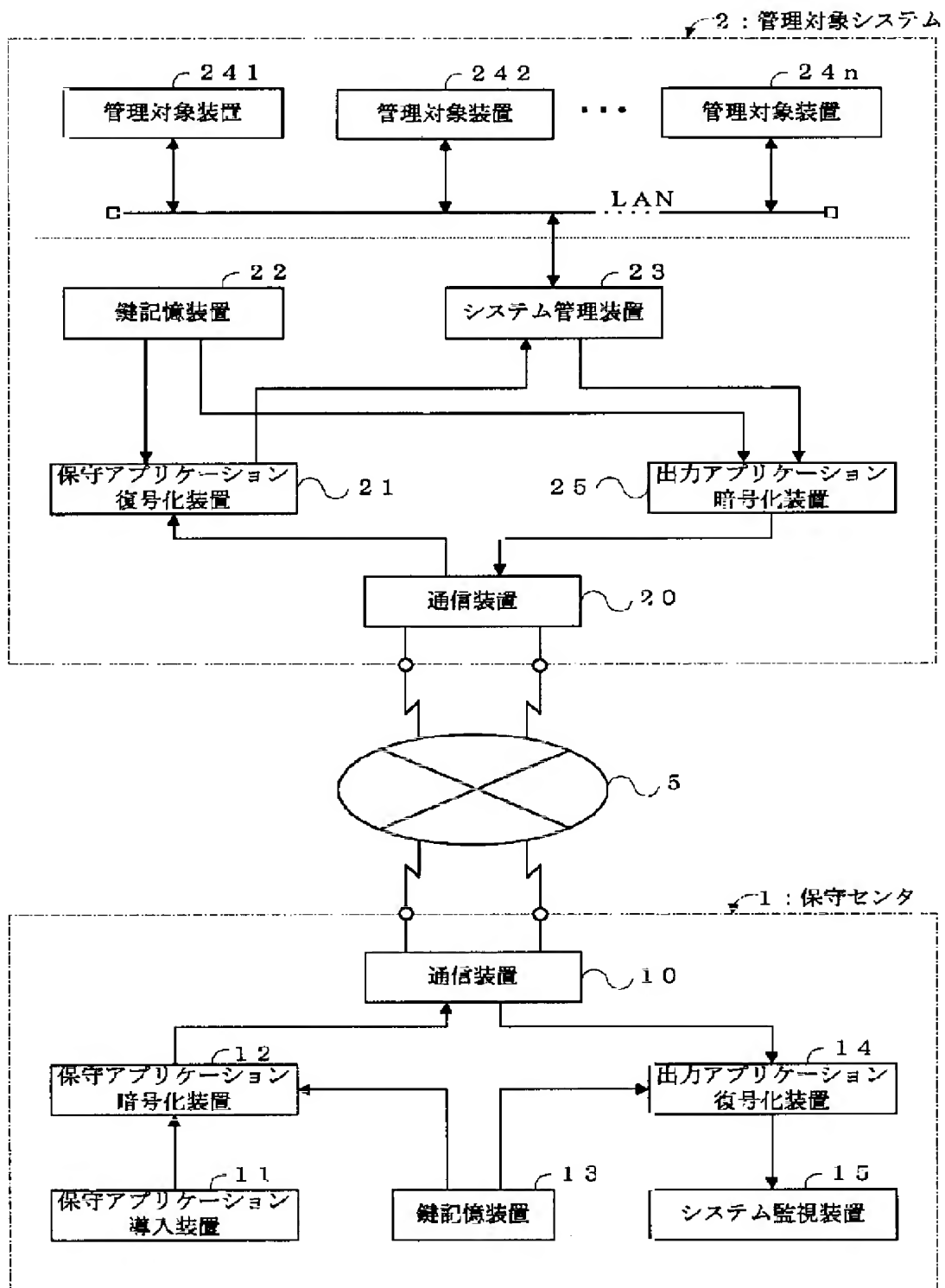
【図11】実施形態にあって出力アプリケーション転送動作の具体的な動作を説明するための図である。

【図12】従来の分散通信システムの遠隔保守管理にかかる構成を示すブロック図である。

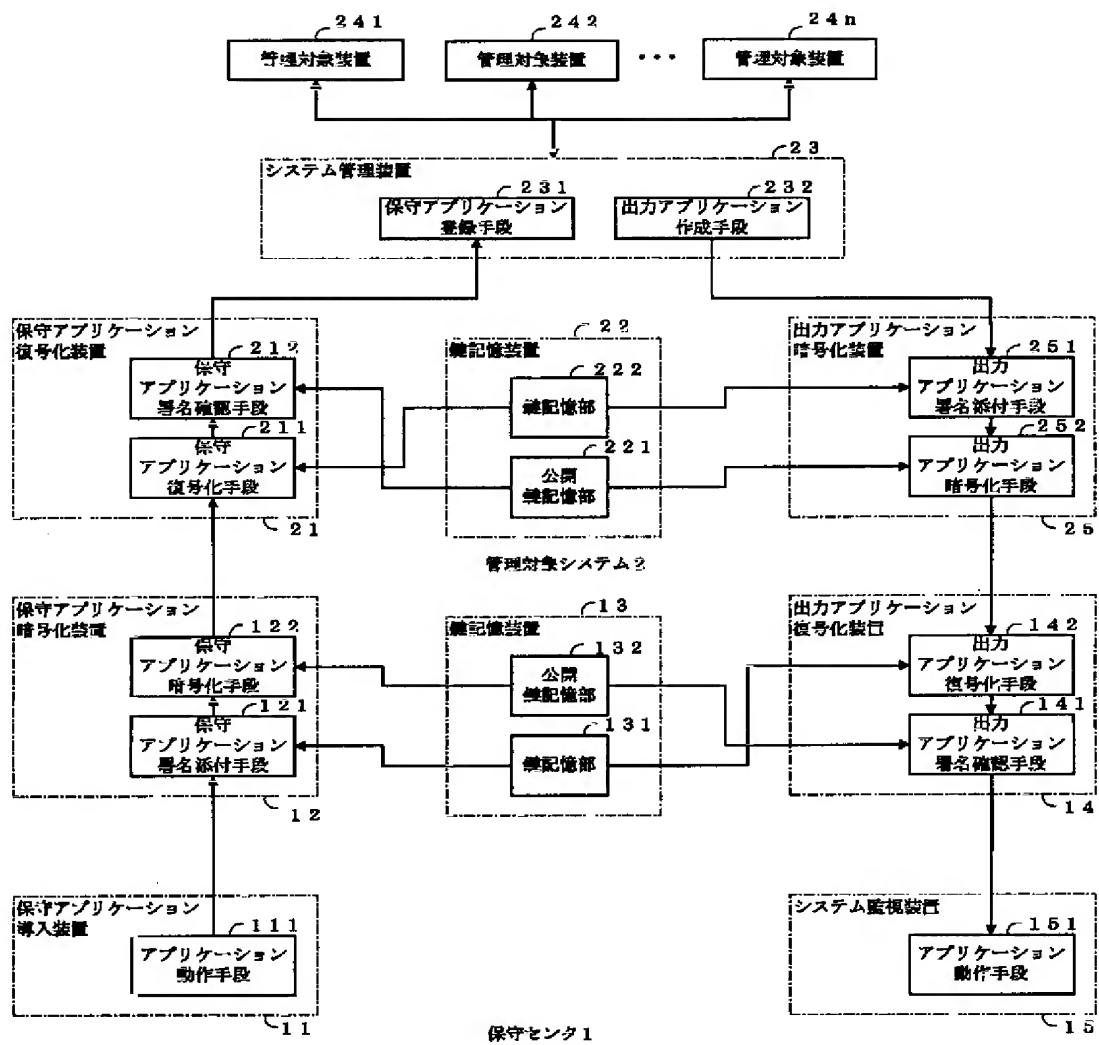
【符号の説明】

- 1 保守センタ
- 2 管理対象システム
- 3 公開鍵記憶装置
- 5 通信ネットワーク
- 10, 20 通信装置
- 11 保守アプリケーション導入装置
- 12 保守アプリケーション暗号化装置
- 13, 22 鍵記憶装置
- 14 出力アプリケーション復号化装置
- 15 システム監視装置
- 21 保守アプリケーション復号化装置
- 23 システム管理装置
- 241, 242...24n 管理対象装置
- 25 出力アプリケーション暗号化装置
- 31 公開鍵記憶部

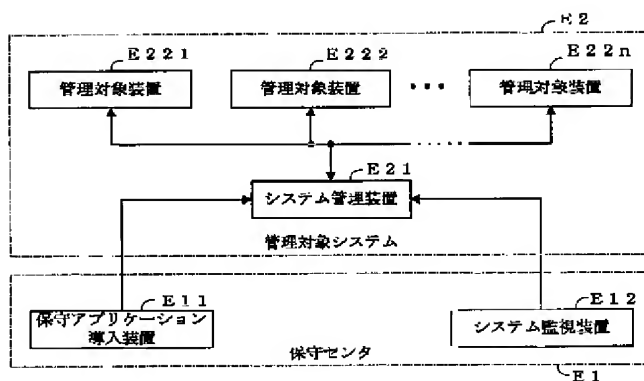
【図1】



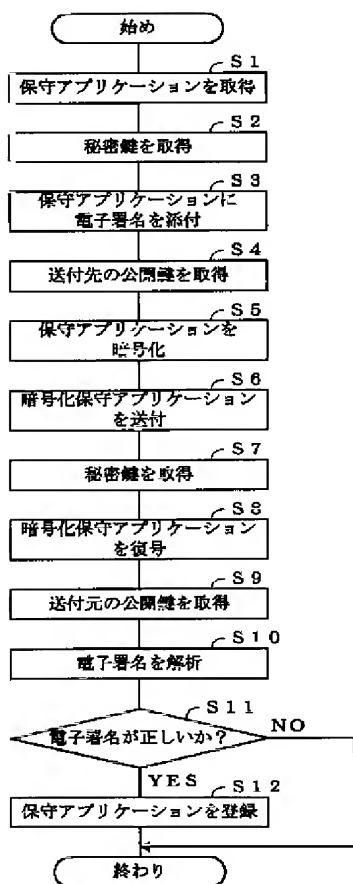
【図2】



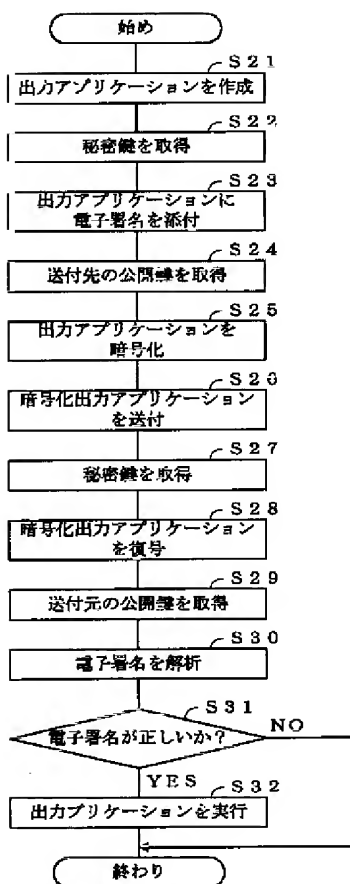
【図12】



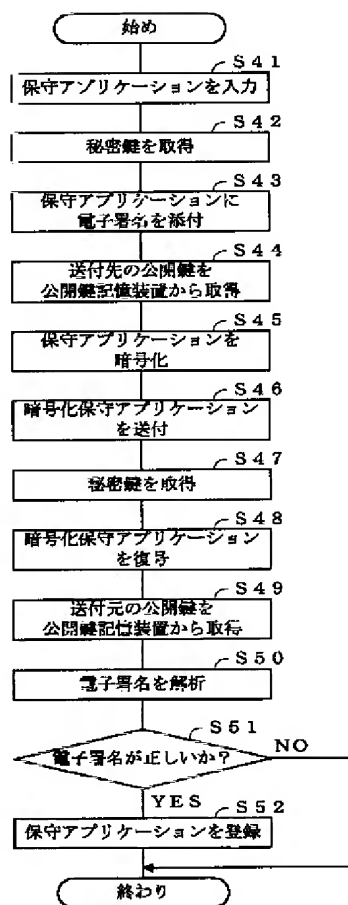
【図3】



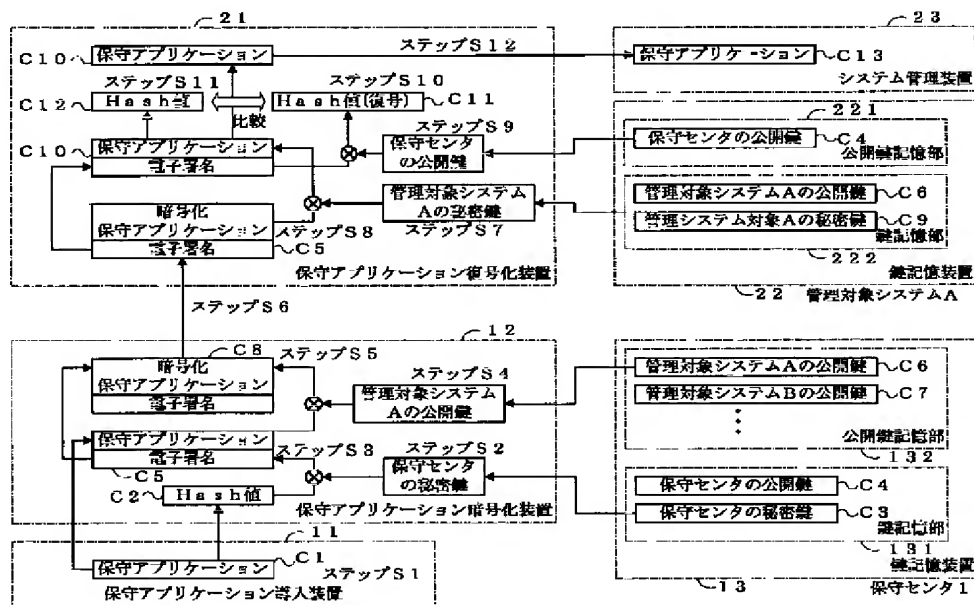
【図4】



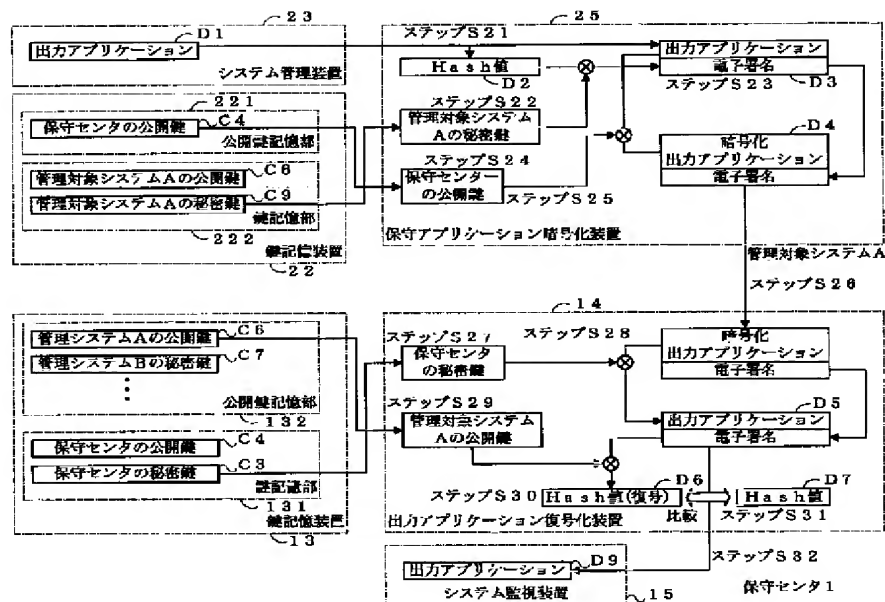
【図8】



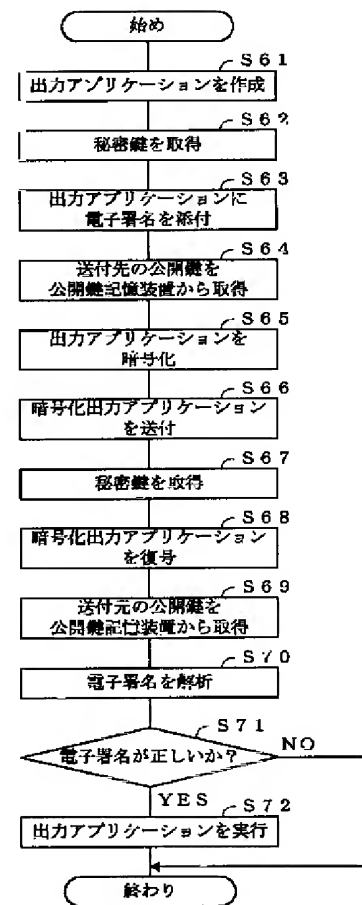
【図5】



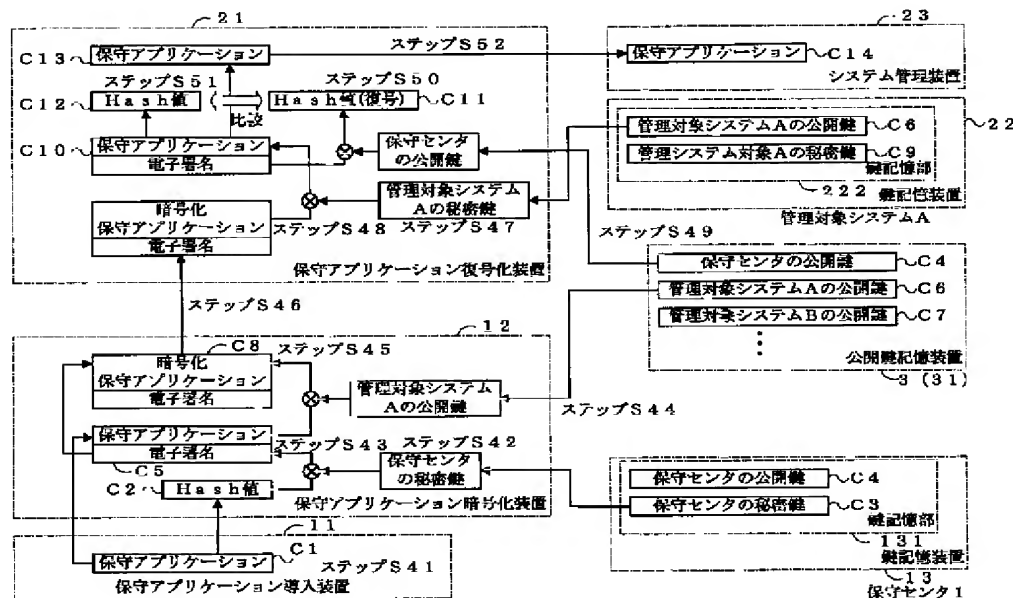
【図6】



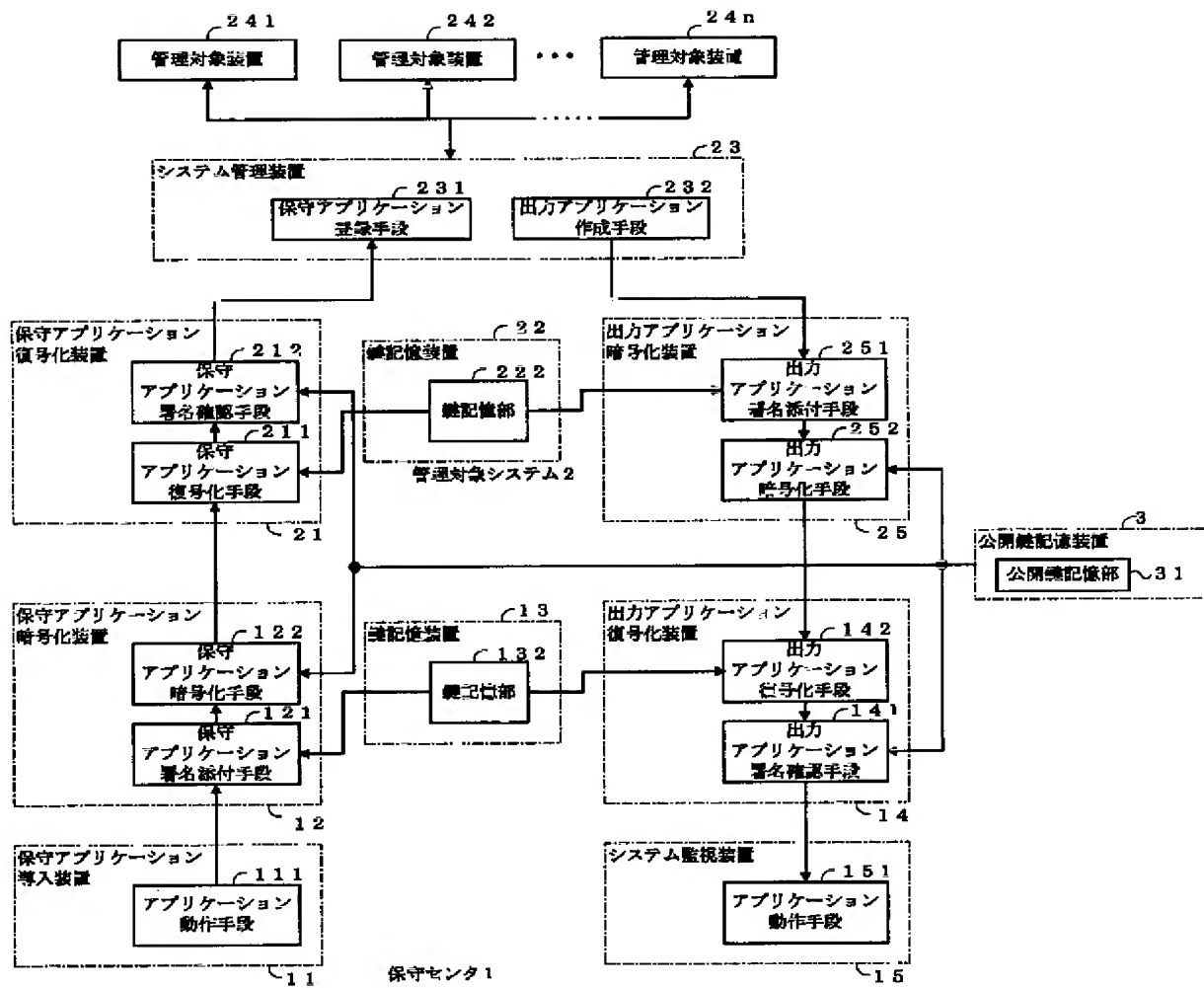
【図9】



【図10】



【図7】



【 図 1 1 】

